UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/490,199	01/24/2000	Michael M. Swift	202267	6863

7590 10/24/2003

Leydig Voit & Mayer LTD
Two Prudential Plaza
Suite 4900
180 North Stetson
Chicago, IL 60601-6780

EXAMINER	
ORTIZ, BELIX M	

ART UNIT	PAPER NUMBER
2175	3

DATE MAILED: 10/24/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/490,199	SWIFT ET AL.	
	Examiner	Art Unit	
	Belix M. Ortiz	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-17 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-17 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on January-24-2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because of the following informalities:

abstract contains more than 150 words. Correction is required.

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

3. Headings appear in bold/underline throughout the disclosed specification.

Headings should not be bold faced and/or underlined.

4. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(h) DETAILED DESCRIPTION OF THE INVENTION.
(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

6. Claims 1 and 2 are rejected under 35 U.S.C. 102(e) as being anticipated by Gutman et al. (U.S. patent No. 6,298,383).

As to claim 1, Gutman et al. teaches a method of enabling a proxy client in a secured network to access a target service on behalf of a user (see column 10, lines 47-79), comprising the steps of:

registering proxy authorization information regarding the user with a trusted security server, the proxy authorization information identifying the proxy client and an extent of proxy authorization (see column 10, lines 51-52);

submitting, by the proxy client, a proxy request to the trusted security server requesting access to the target service on behalf of the user (see column 11, lines 29-31);

comparing, by the trusted security server, the proxy request with the proxy authorization information of the user to determine whether to grant the proxy request (see column 10, lines 53-55);

issuing, by the trusted security server, a data structure containing

authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user (see column 1, lines 65-67 and column 9, lines 32-38).

As to claim 2, Gutman et al. teaches a method wherein the data structure is a ticket containing a session key for use in a session formed between the proxy client and the target service (see column 2, lines 11-17).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gutman et al. (U.S. patent No. 6,298,383) in view of Higley et al. (U.S. patent No. 5,913,025).

As to claim 3, Gutman et al. does not teach, wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

Higley et al. teaches a method for proxy authentication to access a target

(see abstract), in which he teaches wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server (see column 2, lines 18-19).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. to include wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. by the teaching of Higley et al., because wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server, would enable the method to maintain the password or key in secret and the client can feel more secure using the network.

As to claim 4, Gutman et al. does not teach wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

Higley et al. teaches a method for proxy authentication (see abstract), in which he teaches wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired (see column 8, lines 16-18).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. to include wherein

the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. by the teaching of Higley et al., because wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired, would enable the method to have more control of the access to the network and will be more secure for the clients.

As to claim 5, Gutman et al. does not teach wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

Higley et al. teaches a method for proxy authentication (see abstract), in which he teaches wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server (see column 5, lines 17-26).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. to include wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. by the teaching of Higley et al., because wherein the step of submitting the request includes transmitting a

ticket for authenticating the proxy client to the trusted security server, would enable the method to verify the information of the authentication of the client.

As to claim 6, Gutman et al. teaches storing proxy authorization information from a user for authorizing a proxy client to act as a proxy of the user (see column 2, lines 6-10);

receiving a proxy request from the proxy client to access a target service on behalf of the user (see column 11, lines 28-30); and

determining, based on the proxy authorization information of the user, whether to grant the proxy request (see column 12, lines 20-24).

Gutman et al. does not teach a computer-readable medium having computer-executable instructions for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

Higley et al. teaches authorization to access a target (see abstract), in which he teaches a computer-readable medium having computer-executable instructions (see column 4, lines 52-58 and column 5, lines 1-2) for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user (see column 5, lines 17-26).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. to include a computer-readable medium having computer-executable instructions for performing steps:
constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. by the teaching of Higley et al., because a computer-readable medium having computer-executable instructions for performing steps:
constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user, would enable the method to provide a secure network for the clients that want to use the public network.

As to claim 7, Gutman et al. as modified teaches a computer-readable medium having further computer-executable instructions for performing the step of authenticating the user based on a password of the user before storing the proxy authorization information (see Higley et al., column 5, lines 20-21).

As to claim 8, Gutman et al. as modified teaches a computer-readable medium wherein the step of receiving the proxy request includes authenticating

the proxy client based on a ticket issued to the proxy client for communicating with the trusted security server (see Higley et al., column 2, lines 18-19).

As to claim 9, Gutman et al. as modified teaches a computer-readable medium having further computer-executable instructions for performing the step of sending the data structure to the proxy client for presenting to the target service for authentication of the proxy client (see Gutman et al., column 5, lines 1-6).

As to claim 10, Gutman et al. as modified teaches a computer-readable medium wherein the data structure is encrypted with a key shared by the target service and the trusted security server (see Higley et al., column 2, lines 18-19).

9. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Higley et al. (U.S. patent No. 5,913,025) in view of Gutman et al. (U.S. patent No. 6,298,383) and further in view of Shambroom (U.S. patent No. 6,198,824).

As to claim 11, Higley et al. teaches a computer-readable medium having computer executable instructions for a client in a secured network system (see column 4, lines 50-53) to perform the steps of:

constructing an authenticator encrypted with the session key (see column 2, lines 12-22).

Higley et al. does not teach receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service;
decrypting the session key with the shared secret key; and
presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user.

Gutman et al. teaches the integration of authentication authorization and accounting service and proxy service (see abstract), in which he teaches receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service (see column 2, lines 11-25);
decrypting the session key with the shared secret key (see column 2, lines 26-28); and
presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user (see column 2, lines 18-25).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. to include receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service;

decrypting the session key with the shared secret key; and

presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. by the teaching of Gutman et al., because receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service;

decrypting the session key with the shared secret key; and

presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user, would enable the method to be more secure for the user because all the information of each user will be protect from others.

Higley et al. as modified still doesn't teach submitting a proxy request to a trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user;

Shambroom teaches a method for enhancing the security on the network (see abstract), in which he teaches submitting a proxy request to a trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user (see column 5, lines 44-51).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified to

include submitting a proxy request to a trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified by the teaching of Shambroom, because submitting a proxy request to a trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user, would enable the method to know which user is trying to get trough the network and check if he/she have the right authorization to access the network.

As to claim 12, Higley et al. as modified teaches a computer-readable medium wherein the step of submitting the proxy request includes sending a ticket issued to the client for authenticating the client to the trusted security server (see Shambroom, column 5, lines 47-51).

10. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Higley et al. (U.S. patent No. 5,913,025) in view of Vu (U.S. patent No. 5,623,601).

As to claim 13, Higley et al. teaches a computer-readable medium having stored thereon a data structure containing information for proxy authorization (see column 5, lines 17-20), comprising:

a third data field containing data identifying a duration of proxy authorization (see column 8, lines 16-18).

Higley et al. does not teach a first data field containing an identification of a user of a secured network;

a second data field containing an identification of a security principal of the secured network authorized to act as proxy of user; and

a fourth data field containing data specifying a restriction on the proxy authorization.

Vu teaches method that provide a security to private and public network (see abstract), in which he teaches a first data field containing an identification of a user of a secured network (see column 11, lines 39-41);

a second data field containing an identification of a security principal of the secured network authorized to act as proxy of user (see column 16, lines 57-59);

a fourth data field containing data specifying a restriction on the proxy authorization (see column 2, lines 15-23).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. to include a first data field containing an identification of a user of a secured network;

a second data field containing an identification of a security principal of the secured network authorized to act as proxy of user; and

a fourth data field containing data specifying a restriction on the proxy authorization.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. by the teaching of Vu, because a first data field containing an identification of a user of a secured network;

a second data field containing an identification of a security principal of the secured network authorized to act as proxy of user; and

a fourth data field containing data specifying a restriction on the proxy authorization, would enable the method to have more control of the information of the user, easy to find the different data and the network will be more secure.

As to claim 14, Higley et al. as modified teaches a computer-readable medium wherein the data in the third data field specify an expiration date of the proxy authorization (see Higley et al., column 8, lines 16-18).

As to claim 15, Higley et al. as modified teaches a computer-readable medium wherein the data in the fourth data field identify a service of the secured network that the security principal is permitted to access (see Vu column 1, lines 24-27 and column 4, lines 1-4).

11. Claims 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Higley et al. (U.S. patent No. 5,913,025) in view of Vu (U.S. patent No. 5,623,601) as applied above in claim 13 and further in view of Subramaniam et al. (U.S. patent No. 6,081,900).

As to claim 16, Higley et al. as modified teaches a computer-readable medium (see Higley et al., column 4, lines 52-58 and column 5, lines 1-2).

Higley et al. as modified still does not teach wherein the security principal is a client on the secured network.

Subramaniam et al. teaches method and system are provided for secure access to a network (see abstract), in which he teaches wherein the security principal is a client on the secured network (see abstract).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified to include wherein the security principal is a client on the secured network.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified by the teaching of Subramaniam et al., because wherein the security principal is a client on the secured network, would enable the method to be sure that the client has authorization, and that made the network more secure.

12. Claims 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Higley et al. (U.S. patent No. 5,913,025) in view of Vu (U.S. patent No. 5,623,601) as applied above in claim 13 and further in view of Gutman et al. (U.S. patent No. 6,298,383).

As to claim 17, Higley et al. as modified teaches a computer-readable medium (see Gutman et al. column 4, lines 52-58 and column 5, lines 1-2).

Higley et al. as modified does not teach wherein the security principal is a group on the secured network.

Gutman et al. teaches a single database maintained centrally hosts both proxy service and authentication, authorization and accounting (see abstract), in which he teaches wherein the security principal is a group on the secured network (see column 4, lines 31-35).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified to include wherein the security principal is a group on the secured network.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified by the teaching of Gutman et al., because wherein the security principal is a group on the secured network, would enable the method to focus more on the security because have a especial group just for that area.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of art with respect to method of authentication in a secured network in general:

U.S. patent No. 5,983,350 Minear et al.: for teaching a method comprising establishing a security policy on network (see abstract).

U.S. patent No. 6,012,088 Li et al. : for teaching an automatic configuration for internet access (see abstract).

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Belix M. Ortiz whose telephone number is 703-305-7605. The examiner can normally be reached on moday-friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 703-305-3830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

bmo

October 16, 2003.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100